

RANDOM NUMBERS GENERATOR

Patent Number: JP6051957
Publication date: 1994-02-25
Inventor(s): HASHIMOTO TOKUO; others: 01
Applicant(s): RICOH CO LTD
Requested Patent: ☐ JP6051957
Application Number: JP19920224702 19920731
Priority Number(s):
IPC Classification: G06F7/58
EC Classification:
Equivalents:

Abstract

PURPOSE: To generate a random numbers string with different arrangement of pulse string by switching the feedback position of a linear feedback shift register(LFSR) after the random numbers string is generated extending over a certain period decided in advance.

CONSTITUTION: The LFSR is comprised of a shift register 401 of seven bits, an exclusive OR circuit 404, and a selector 402 which selects the feedback position. Respective bit data r1-r7 of the shift register 401 are taken out in parallel, and binary random numbers b0-b6 in which a shift-in side is set as an LSB, and a shift-out side as an MSB can be obtained. Furthermore, a two-bit binary counter 403 is connected to the selector 402, and the counter 403 receives contents in sequence of 00 01 10 11 00 corresponding to the input of a count clock 407, and the bit data r1 is selected for 00, and r6 for 01, and r4 for 10, and r3 for 11, then, they are fed back. Therefore, the arrangement of a pulse can be changed by changing the feedback position of the LFSR.

Data supplied from the esp@cenet database - I2

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-51957

(43)公開日 平成6年(1994)2月25日

(51)Int.Cl.⁵

G 0 6 F 7/58

識別記号

庁内整理番号

F I

技術表示箇所

A 9188-5B

審査請求 未請求 請求項の数4(全 7 頁)

(21)出願番号

特願平4-224702

(22)出願日

平成4年(1992)7月31日

(71)出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72)発明者 橋本 篤男

東京都大田区中馬込1丁目3番6号 株式会社リコー内

(72)発明者 榎本 杉高

東京都大田区中馬込1丁目3番6号 株式会社リコー内

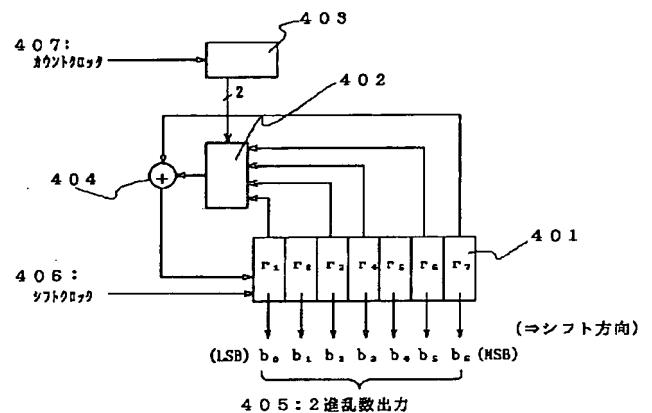
(74)代理人 弁理士 鳥居 洋

(54)【発明の名称】 乱数発生装置

(57)【要約】

【目的】 乱数発生装置に関し、パルス列の並びが異なる乱数列を発生することができる乱数発生装置を提供することを目的とする。

【構成】 n次の最大周期列信号を生成するLFSRを備えた乱数発生装置において、あらかじめ定められた期間にわたって乱数列を発生した後、カウンタ403と、カウンタ403の内容に対応して前記LFSRのシフトレジスタ501のフィードバック位置を切り替えるセレクタ502からなり、予め定められた期間にわたって乱数列を発生した後、前記LFSRのフィードバック位置を切り替える手段を設ける構成とする。



【特許請求の範囲】

【請求項 1】 n 次の最大周期列信号を生成する第一のリニアフィードバックシフトレジスタ（以後、リニアフィードバックシフトレジスタを LFSR と略記する。）を備えた乱数発生装置において、あらかじめ定められた期間にわたって乱数列を発生した後、前記 LFSR のフィードバック位置を切り替える手段を設けたことを特徴とする乱数発生装置。

【請求項 2】 上記手段が、カウンタと、カウンタの内容に応じて LFSR のフィードバック位置を切り換えるセレクトとを備えることを特徴とする請求項 1 に記載の乱数発生装置。

【請求項 3】 上記手段が、 m ビットのシフトレジスタと、該シフトレジスタに格納されたビットデータに従って前記 LFSR のフィードバック位置を切り換えるセレクトとを備えることを特徴とする請求項 1 に記載の乱数発生装置。

【請求項 4】 上記手段が、最大周期列信号を生成する第二の LFSR と、前記第二の LFSR から発生させた 2 値乱数により前記第一の LFSR のフィードバック位置を切り替えるセレクトとを備えることを特徴とする請求項 1 に記載の乱数発生装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、パルス密度変調されたランダムパルス列を生成する装置に用いられる乱数発生装置に関する。

【0002】

【従来の技術】 従来、信号処理装置として、数値を 2 値パルス列（ここでは、便宜上 “1” と “0” の 2 値で表現されるパルス列とする）の時間当たりの “1” 又は “0” のパルスの数、即ちパルス密度で表現して、演算処理を行なうものがある。

【0003】 例えば、図 1 に示される様に、パルス列で表現された数値の積は、2 値パルス列の論理積で求めることができる。1/4 のパルス密度を持つパルス列 a と 1/2 のパルス密度を持つパルス列 b の論理積をとるパルス列 c になりそのパルス密度は、1/8 となる。精度に注意すれば簡単なデジタル回路で、演算系を構成することが可能である。この場合の演算精度は、パルス列の長さとは、“1” の位置の不規則度によって決まることは明かである。

【0004】 このような用途に供される、2 値パルス列を得るために一様乱数を発生する乱数源と比較器を用い

(2 値乱数列式)

(a) 特殊多項式 $1 + X + X^7$ (フィードバック位置；1 番目、7 番目)

) M 系列 100000011111101010100110011101110100101100011011101101
0110110010010001110000101111001010111001101000100111100
010100001100000

る方法がある。例えば、基準クロック 127 個分の長さを持つパルス列でパルス密度が、 $10/127$ であるようなパルス列を得るためには、1 から 127 までの一様乱数を順次発生させ所望の数値 10 と比較器で比較し、再生された乱数が 1 から 10 ならば、“1” のパルスを出力し、11 から 127 ならば、“0” のパルスを出力すれば、所望のパルス列を得ることができる。乱数源としては従来、物理雑音を使う方法等が用いられていたが、再現性がない、特性の制御が難しい等の理由により、最近では、簡単なデジタル回路で構成可能であり、良質な 2 値乱数列を得ることができる LFSR が良く用いられる。LFSR は、例えば図 2 に示すようにシフトレジスタの一部のビットをフィードバックしてその排他論理和をとって再びシフトインさせるもので、フィードバック位置を注意深く選ぶと、最大周期列信号と呼ばれる 2 値乱数列が得られる。 p 段 LFSR では最大で “ $2^p - 1$ ” の周期を持つ 2 値数列が得られるが、この中で最大の周期を持つものが、最大周期列信号である。

【0005】 例えば、7 段の LFSR で最大周期列信号の得られる回路構成は、図 3 (a) ~ (d) に示される 4 種類が存在する。回路の左側に記された式 1 ~ 4 は、特性多項式とよばれ、フィードバック位置を示すものである。図 3 (a) ~ (d) に示される LFSR に最大周期である 127 個のクロックをあたえて発生させた 2 値乱数列を 2 値乱数列式 (a) ~ (d) に示す。ここでは、1000000 (2 進) を LFSR の初期値として順次シフトアウトされる 2 値数列を示している。

【0006】 この 2 値乱数列から、注意深く決めた一定の間隔で取りだして、並列に並べることにより、2 進数乱数列を得られる。例えば、前述した 1 ~ 127 の乱数列を得るためには、7 段の LFSR のうち最大周期信号を発生するものを用意して、LFSR の各ビットを並列に取りだして、7 ビットの乱数列とすればよい。これは、最大周期信号列から間隔 1 で順次 7 ビット取りだすことに相当する。

【0007】 図 3 (a) ~ (d) に示される LFSR で、シフトイン側のビットを LSB、シフトアウト側のビットを MSB とし、LFSR の初期値を 64 (10 進) とすると乱数列式 (a) ~ (d) に示す乱数列が得られる。1 ~ 127 の数の出現は、不規則であり前述した一定のパルス密度のランダム 2 値パルス列の生成に使用することができる。

【0008】

3

4

(b) 特殊多項式 $1 + X^6 + X^7$ (フィードバック位置; 6 番目、7 番目)

M系列 10000001000001100001010001111001000101100111010100111110
 10000111000100100110110101101111011000110100101110111001
 100101010111111

(c) 特殊多項式 $1 + X^4 + X^7$ (フィードバック位置; 4 番目、7 番目)

M系列 10000001000100110001011101011011000001100110101001110011
 1101101000010101011111010010100011011100011111100001110
 111100101100100

(d) 特殊多項式 $1 + X^3 + X^7$ (フィードバック位置; 3 番目、7 番目)

M系列 1000000100100110100111101110000111111000111011000101001
 01111101010100001011011110011100101011001100000110110101
 110100011001000

【 0 0 0 9 】

(乱数列式)

(a) $1 + X + X^7$

乱数列 64 1 3 7 15 31 63 127 126 125 122 117 106 85 42 84 41
 83 38 76 25 51 103 78 29 59 119 110 93 58 116 105 82
 37 75 22 44 88 49 99 70 13 27 55 111 94 61 123 118 109
 90 53 107 86 45 91 54 108 89 50 100 73 18 36 72 17 35
 71 14 28 56 112 97 66 5 11 23 47 95 62 124 121 114 101
 74 21 43 87 46 92 57 115 102 77 26 52 104 81 34 68 9
 19 39 79 30 60 120 113 98 69 10 20 40 80 33 67 6 12 24
 48 96 65 2 4 8 16 32

(b) $1 + X^6 + X^7$

乱数列 64 1 2 4 8 16 32 65 3 6 12 24 48 97 66 5 10 20 40 81 35
 71 15 30 60 121 114 100 72 17 34 69 11 22 44 89 51 103
 78 29 58 117 106 84 41 83 39 79 31 62 125 122 116 104
 80 33 67 7 14 28 56 113 98 68 9 18 36 73 19 38 77 27 54
 109 90 53 107 86 45 91 55 111 94 61 123 118 108 88 49
 99 70 13 26 52 105 82 37 75 23 46 93 59 119 110 92 57
 115 102 76 25 50 101 74 21 42 85 43 87 47 95 63 127 126
 124 120 112 96

(c) $1 + X^4 + X^7$

乱数列 64 1 2 4 8 17 34 68 9 19 38 76 24 49 98 69 11 23 46 93
 58 117 107 86 45 91 54 108 88 48 96 65 3 6 12 25 51 102
 77 26 53 106 84 41 83 39 78 28 57 115 103 79 30 61 123
 118 109 90 52 104 80 33 66 5 10 21 42 85 43 87 47 95 62
 125 122 116 105 82 37 74 20 40 81 35 70 13 27 55 110 92
 56 113 99 71 15 31 63 127 126 124 120 112 97 67 7 14 29
 59 119 111 94 60 121 114 101 75 22 44 89 50 100 73 18
 36 72 16 32

(d) $1 + X^3 + X^7$

乱数列 64 1 2 4 9 18 36 73 19 38 77 26 52 105 83 39 79 30 61
 123 119 110 92 56 112 97 67 7 15 31 63 127 126 124 120
 113 99 71 14 29 59 118 108 88 49 98 69 10 20 41 82 37
 75 23 47 95 62 125 122 117 106 85 42 84 40 80 33 66 5

11 22 45 91 55 111 94 60 121 115 103 78 28 57 114 101
 74 21 43 86 44 89 51 102 76 24 48 96 65 3 6 13 27 54
 109 90 53 107 87 46 93 58 116 104 81 35 70 12 25 50
 100 72 17 34 68 8 16 32

【 0 0 1 0 】

【発明が解決しようとする課題】しかしながら、このような L F S R を使った乱数生成装置を用いて、繰り返しランダム 2 値パルス列を発生せる場合、L F S R の構造が決まれば、パルス列内では、“ 1 ” の並びがランダムであるが、繰り返し発生するパルス列どうしを比べると、毎回同じパルス並びとなり、不都合である。

【 0 0 1 1 】本発明は、繰り返し乱数列を発生させる時に、パルス列の並びが異なる乱数列を発生することができる乱数発生装置を提供することを目的とする。

【 0 0 1 2 】また、本発明は、繰り返し乱数列を発生させる時に、毎回ランダムな種類の乱数列を簡単に発生させることができる乱数発生装置を提供することを目的とするものである。

【 0 0 1 3 】

【課題を解決するための手段】この発明による第 1 の乱数発生装置は、n 次の最大周期列信号を生成する第一の L F S R を備えた乱数発生装置において、上記の目的を達成するため、あらかじめ定められた期間にわたって乱数列を発生した後、前記 L F S R のフィードバック位置を切り替える手段を設けたことを特徴とする。

【 0 0 1 4 】この発明による第 2 の乱数発生装置は、上記第 1 の乱数発生装置において、上記手段が、カウンタと、カウンタの内容に応じて L F S R のフィードバック位置を切り換えるセクタとを備えることを特徴とする。

【 0 0 1 5 】この発明による第 3 の乱数発生装置は、上記第 1 の乱数発生装置において、上記手段が、m ビットのシフトレジスタと、該シフトレジスタに格納されたビットデータに従って前記 L F S R のフィードバック位置を切り替えるセクタとを備えることを特徴とする。

【 0 0 1 6 】この発明による第 4 の乱数発生装置は、上記第 1 の乱数発生装置において、上記手段が、最大周期列信号を生成する第二の L F S R と、前記第二の L F S R から発生させた 2 値乱数により前記第一の L F S R のフィードバック位置を切り替えるセクタとを備えることを特徴とする。

【 0 0 1 7 】

【作用】L F S R のフィードバック位置を変化させると、繰り返し発生される乱数列のパルスの並びが変化する。

【 0 0 1 8 】なお、L F S R を備えた乱数発生装置においてパルスの並びが異なる乱数列を発生させるためには、本発明の方法の他に、L F S R の初期値を変更する方法も考えられる。

【 0 0 1 9 】

【実施例】本発明の一実施例に係る乱数発生装置を図面に基いて具体的に説明すれば、以下の通りである。

【 0 0 2 0 】図 4 の回路図に示すように、7 ビットのシフトレジスタ 4 0 1 と、排他的論理和回路 4 0 4 と、フィードバック位置を選択するセクタ 4 0 2 とで L F S R が構成される。

【 0 0 2 1 】このシフトレジスタ 4 0 1 の各ビットデータ r 、 r …… r を並列に取り出し、シフトイン側を L S B シフトアウト側を M S B とした 2 進数乱数 (b_0 , b_1 , b_2 , b_3 , b_4 , b_5 , b_6) を得る。

【 0 0 2 2 】さらに、セクタ 4 0 2 には 2 ビットバイナリカウンタ 4 0 3 が接続され、カウンタ 4 0 3 はカウンタクロック 4 0 7 の入力に応じて $00 \rightarrow 01 \rightarrow 10 \rightarrow 11 \rightarrow 00$ の順で内容を受け取り、図 5 の対比図に示すように、“ 0 0 ” に対しては r_1 、“ 0 1 ” に対しては r_6 、“ 0 1 ” に対しては r_4 、“ 1 1 ” に対しては r_3 を選択して、フィードバックするようにしている。

【 0 0 2 3 】例えば、初期値としてカウンタ 4 0 3 には“ 0 0 ”を、シフトレジスタ 4 0 1 には“ 0 0 0 0 0 1 ”のデータを設定した場合、フィードバックは r_1 が選択されるので、順次この状態からシフトクロック 4 0 6 にクロックを 1 2 7 回入れることにより、乱数列式 (a) に示す乱数列 6 4、1、3、7、15、31、… が得られる。次に、カウンタクロック 4 0 7 にクロックを少なくとも 1 回入れる。例えば 1 回だけ入れるとカウンタ 4 0 3 は 1 つ進み“ 0 0 ”から“ 0 1 ”に代わり、フィードバックは r_1 から r_6 に切換わる。

【 0 0 2 4 】この状態から再びシフトクロック 4 0 6 にクロックを 1 2 7 回入れると、今度は乱数列式 (b) に示す乱数列 6 4、1、2、4、8、16、32、… が得られ、前回とは異なったものとなる。

【 0 0 2 5 】カウンタクロック 4 0 7 に入れるクロックはある一定周期毎に少なくとも 1 回出力する様に制御すればよい、カウンタ 4 0 3 は 2 b i t でなくともよく n ビットのうちの m ビットをデコードして、セクタ 4 0 2 を制御してもよい。

【 0 0 2 6 】乱数発生に用いる L F S R は実施例では 7 ビットであるが、他のビット数であってもよい。さらに 7 ビット以外ならば可能なフィードバック位置は、4 ケ所以外となるかも知れないのでセクタ 4 0 2 で選択するフィードバック位置と、フィードバック数は実施例以外のものでもよい。

【 0 0 2 7 】このように本実施例では乱数列を繰り返し発生する毎に、図 5 に示されるように、フィードバック位置をサイクリックに更新し、前回とは異なる種類の乱数列を得ることができる。

【0028】図6は、本発明の他の実施例に係る乱数発生装置の回路図であり、この装置は7ビットのシフトレジスタ501と、排他的論理和回路504と、フィードバック位置を切り換えるセレクタ502とからなる7ビットの第1LFSR505を備える。

【0029】また、セレクタ502には2ビットのシフトレジスタ503が接続され、内容に応じてシフトレジスタ501のフィードバック位置が切り換わるよう構成されている。シフトレジスタ503の内容が"00"ならばr11が、"01"ならばr16が、"10"ならばr14が、"11"ならばr13が各々選択される。

【0030】さらに、シフトレジスタ503のシフト入力端子には、第2LFSR506のシフトアウト端子が接続され、LFSR506のシフトアウトデータをシフトレジスタ503に入力できるよう構成されている。LFSR506のフィードバック位置はr31からのフィードバックに固定されており、2値乱数列式(a)に示される最大周期列信号を発生する。

【0031】シフトレジスタ503には初期値として、例えば"11"が設定される。さらに、シフトレジスタ501には、初期値として"0000001"のデータを設定する。さらにLFSR506には初期値として、"1011100"を設定する。シフトレジスタ503の内容が"11"でLFSR505のフィードバックはr13が選択される。順次この状態からシフトクロック508にクロックを127回入れることにより、2値乱数列として64、1、2、4、9、18、36…が得られる。

【0032】次にシフトクロック509にクロックを少なくとも1回入れる。例えば1回だけ入れたとすると、シフトレジスタ503の内容は"11"から"01"に変わりLFSR505のフィードバック位置はr13からr16に切り換わる。この状態から再びシフトクロック508にクロックを127回入れると、今度は、64、1、2、4、8、16、32…の乱数列が得られ、前回とは異なった乱数列が得られる。以下、乱数列に繰り返し発生することに図7の対比図に示すようにシフトレジスタ503の内容が"01"→"00"→"10"→…のように変更され、前回とは異なる種類の乱数列が得られることになる。

【0033】さらに、LFSR506で発せられる2値乱数列は最大周期列信号であり、したがって、シフトレジスタ503の内容は繰り返し毎に、毎回ランダムなものとなる。

【0034】本実施例ではLFSR505、509とも

7段のものにしたが他の段数でも良い。さらにLFSR506のフィードバック位置は他の位置でもよい。

【0035】

【発明の効果】この発明の第1の乱数発生装置によれば、LFSRのフィードバック位置を切り変えることによりパルスの並びが異なる乱数列を出力させることができる。

【0036】この発明の第2の乱数発生装置によれば、カウンタの内容を変化させ、カウンタの内容に応じてセレクタでLFSRのフィードバック位置を切り変えることによりパルスの並びが異なる乱数列を出力させることができる。

【0037】この発明の第3の乱数発生装置によれば、シフトレジスタのビットデータを変化させることにより、このビットデータの内容に応じてセレクタでLFSRのフィードバック位置を切り換え、パルスの並びが異なる乱数列を出力させることができる。

【0038】この発明の第4の乱数発生装置によれば、第2のLFSRから発生させた2値乱数を変化させることにより、セレクタで第1のLFSRのフィードバック位置を切り換え、第1のLFSRからパルスの並びが異なる乱数列を出力させることができる。

【図面の簡単な説明】

【図1】パルス密度方式の演算の原理図である。

【図2】LFSRの構成図である。

【図3】フィードバック位置によるLFSRの出力変化を示す説明図である。

【図4】本発明の構成図である。

【図5】カウンタの内容、フィードバック位置及び特性多項式の対応関係を示す対比図である。

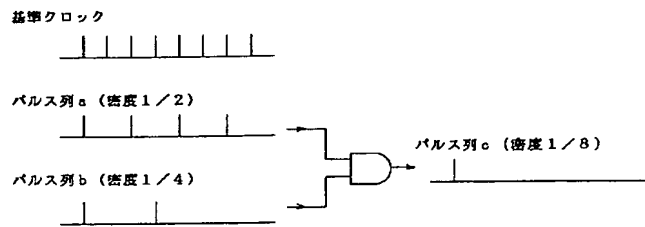
【図6】本発明の構成図である。

【図7】第2LFSRの最大周期信号、第2LFSRのビットデータ、シフトレジスタの内容及び状態の対応関係を示す対比図である。

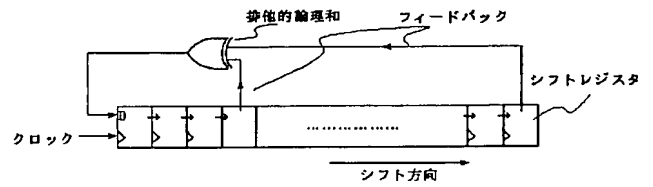
【符号の説明】

401 シフトレジスタ
402 セレクタ
403 カウンタ
404 排他的論理和回路
501 シフトレジスタ
502 セレクタ
503 シフトレジスタ
504 排他的論理和回路
505 第1LFSR
506 第2LFSR

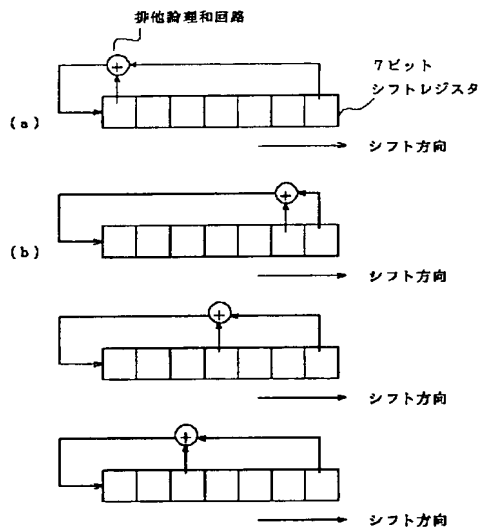
【図 1】



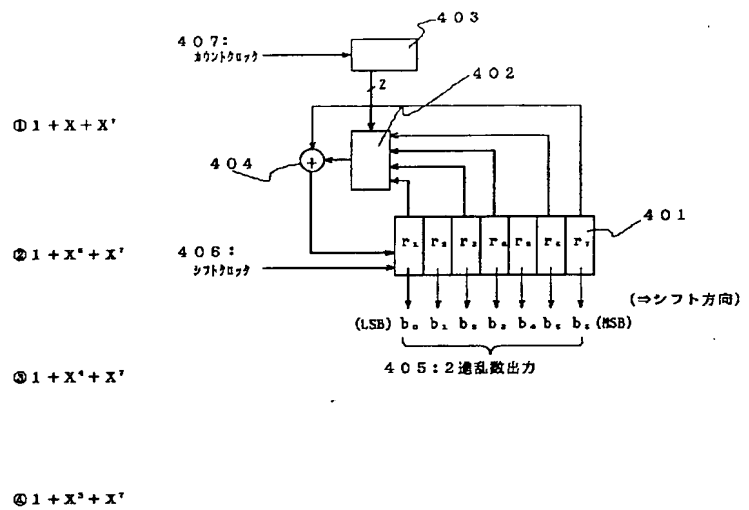
【図 2】



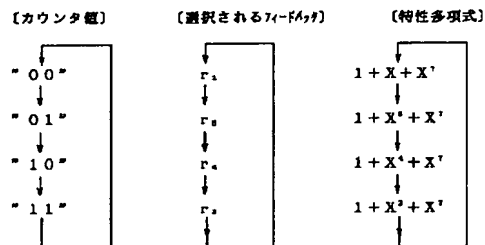
【図 3】



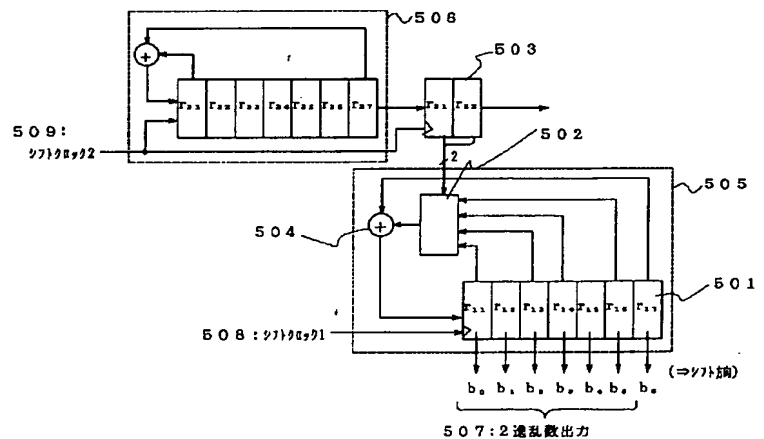
【図 4】



【図 5】



【図 6】



【図 7】

